2 Technical Reference Model (TRM) and Standards Profiles

2.1 Foreword to TRM and Standards Profiles

2.1.1 Introduction to the TRM and Standards Profiles

The Technical Reference Model (TRM) and Standards Profiles (both technical and security) comprise a vital crosscutting element for FEMA IT systems, affecting virtually all components of the FEMA Enterprise Architecture. Increased use of open systems standards will enable interoperability, portability, and scaleability in IT systems across FEMA. Standards must be consistent and uniformly applied throughout the Agency and across the enterprise. Standards form the basis for development of re-usable components of the FEMA Enterprise Architecture, and the CIO and IRB will use established standards to guide and constrain IT asset acquisitions in the future. There are a number of technical, operational, and managerial issues associated with the application of standards for the creation, management, and use of electronic documents and data across the enterprise.

2.1.2 Background of the TRM and Standards Profiles

This *FEMA IT Architecture* document provides the first formal Technical Reference Model (TRM) and set of standards profiles developed by FEMA. As noted in Section 1, the FEMA ITS Directorate has indicated that an internationally-accepted, open systems, disciplined, and standards-based IT architecture will best meet FEMA's needs for designing and developing future information systems, for re-engineering legacy systems, and for achieving future integration and interoperability among systems across the broad and distributed FEMA enterprise. The development of a formal TRM represents an important opportunity for FEMA to increase interoperability, redundancy, portability, and security across FEMA IT systems, and to do so in an open systems fashion. A standards based TRM also simplifies user training and support.

Heretofore, the common practice of defining a standard at FEMA has been largely a matter of declaring that all organizational entities use the same standard tool, such as cc:Mail or Microsoft Word or Power Point. This approach clearly has its pros and cons. At one level, it is very expedient to declare a tool to be a standard, and *pretty much* assures that FEMA organizational elements will be able to instantly interchange and use data files among each other via electronic means. Despite the good intentions of national and international open systems standards organizations, FEMA observes that, unless there is a critical mass of vendor support for an open systems standard and a uniform method of implementing the standard (e.g., a widely-accepted application portability profile (APP)), competitive proprietary approaches will tend to win out in the marketplace.

FEMA does not have the resources to develop its own suite of tools to implement open systems-compliant tools in lieu of appreciable vendor and industry interest and support. Furthermore, FEMA does not have the resources to develop standards profiles for use across the emergency management community. To achieve interoperability, FEMA strongly prefers to be a consumer or user of existing profiles.

On the other hand, the approach of declaring a tool, system, or application as the FEMA standard has tended to lock FEMA and other Federal agencies that have also done so into certain vendors and their proprietary file formats. The major concerns with this approach are:

- Achieving interoperability with FEMA's external business partners, who may be using a different tool, is problematic. Achieving cross-agency and FEMA business partner consensus on tools continues to be a very difficult proposition.
- FEMA, like other Federal agencies, has virtually no control or influence over the tool vendor and the file format definition. There is always the concern that the file format might become an unsupported orphan and make it difficult for FEMA to migrate the data to a new tool without risking loss of data and document integrity.
- The tool vendor may go out of business or be sold to a competitor and the file format become an orphan or be completely re-engineered to not be reverse compatible.
- FEMA has little or no control over the standard tool releases or versions. Even if FEMA partners are using the same standard tool, they may be using different versions, and the data interchange may fail at that level.
- Lastly, the file and data formats for many industry standard and proprietary formats are not supported for long-term archival storage and retrieval purposes. Additionally, any translation to an acceptable archival format risks loss of document and data integrity. This situation is a common problem for other Federal agencies.

Notwithstanding the above, FEMA supports the implementation of open systems standards as a basis for achieving interoperability, transportability, and long-term data integrity. FEMA also notes that otherwise worthy open systems standards will languish if they do not receive a critical mass of support and interoperability testing from vendors. Similarly, vendors will only develop tools if they perceive a customer base and demand for the product. Thus, specifying an open systems standard helps to "make it be known" that FEMA and other agencies are ready customers and supporters of open systems.

In implementing open systems standards, FEMA desires the widest possible ability to interchange information. This implies that the standards and the supporting tools be tested and viable in large-scale, enterprise-wide operations. If only one vendor implements the standard, the information still may not be interchangeable across systems, especially if the vendor later drops the product. Even if two vendors implement the open systems standard just as Microsoft and Netscape have done by interpreting the requirements for HTML slightly differently in their Web browsers, there is still no guarantee of interoperability. Figure 2-1 illustrates the target concept for developing and implementing open systems.

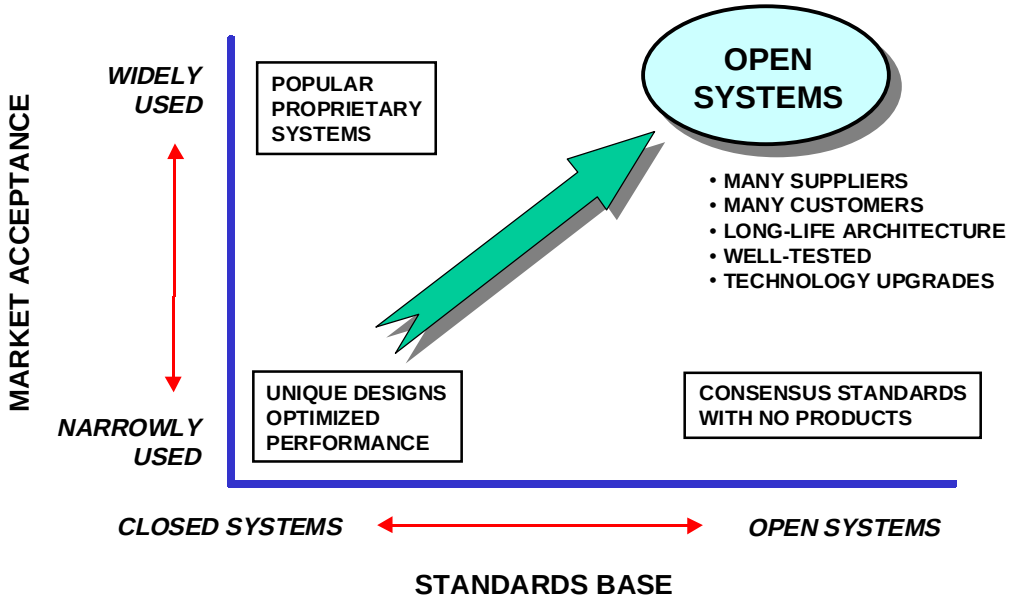

Figure 2-1. FEMA Target Concept for Implementing Open Systems Standards

As a practical matter for this TRM, FEMA will place appropriate emphasis on adopting open systems approaches, but also recognizes the operational need to specify the use of a particular standard tool if no fully open systems approach be viable and tested.

2.1.3 Terms and Definitions

This section provides working terms and definitions for the following:

- **Technical Reference Model (TRM)** – A TRM is a model that provides the basic ground rules, set of standards, or building code for designing, developing, implementing, testing, and integrating IT systems. The TRM identifies and describes the basic information services (such as data base services, document management services, security services, etc.) at a high level, and how they ought to be designed and constructed in a uniform and standardized manner.
- **Standards Profile** – A standards profile defines how a particular standard such as an open systems standard, an industry standard, or a standard tool needs to be customized or tailored to support interchange or interoperability. A profile recognizes that all major standards generally need to be customized or profiled through establishment of user conventions. These profiles or user conventions are frequently referred to as Application Portability Profiles (APPs).
- **Standard Tool** – A standard tool is defined as an IT tool, system, or application that FEMA has determined to meet operational requirements and is mandated for use in IT systems. A standard tool is part of the *FEMA IT Architecture*.
- **Security Services Model** – A security services model is the Technical Reference Model for security services (such as access controls, confidentiality, fault tolerance, originator authentication, etc.).
- **Security Standards Profile** – A security standards profile is the same as a standards profile except that it refers to security standards.

2.1.4 Goals and Objectives

Table 2-1 identifies the goals and objectives of the FEMA TRM and Standards Profiles.

Table 2-1. Goals and Objectives

Goals and Objectives	Description of Development Opportunity
Interoperability	Promotes interoperability through defining the basic building code or building blocks for systems and makes the requirements be known to FEMA's enterprise partners, developers, and integrators.
Stability	Provides a stable base for development of IT systems.
Re-use	Promotes re-use through establishment of a standardized architectural components that are mandated for use in new developments and re-engineered or re-hosted systems.
Portability	Promotes portability through emphasis on selecting open systems approaches wherever practicable.
Longevity of data	Helps ensure longevity of data by formally defining and/or profiling a standard. If a vendor or a standard tool goes out of business or is withdrawn, the definition and profile of the standard can be used to recover and/or read the legacy data.
Cost effectiveness	Promotes cost effectiveness through establishment of common approaches for re-use.
Compatibility with NIST TRM	To promote interoperability across Federal agencies, the FEMA TRM is compatible to the maximum extent practicable with the NIST TRM.
Year 2000 compliance	Firmly establishes the architectural baseline and ground rules for achieving Year 2000 compliance. All FEMA architectural components shall be Year 2000 compliant.

2.1.5 CIO Directives for Application of the TRM and Standards Profiles in FEMA IT Systems

To achieve the goals of interoperability and consensus across the emergency management community, FEMA will use and exploit existing standards and proven standards profiles, wherever practicable. The following directives and guidelines shall apply:

- FEMA is committed to employment of open systems standards wherever practicable to achieve the goals and objectives identified above. An open systems life-cycle approach that is workable and viable is strongly preferred over proprietary approaches, which might be more expedient.
- The Technical Reference Model and Standards Profiles shall be applied to the development of both enterprise-wide IT systems and standalone, program-centric systems to the maximum extent practicable.
- The *FEMA IT Architecture* (including the TRM and Standards Profiles) is considered a living document. Updates and revisions will be made as required. The *FEMA IT Architecture* document shall be under strict configuration management and control.
- Consistent with the architectural principles in Appendix H , any FEMA organizational element or established business partner may request waivers, deviations, or exceptions to the *IT Architecture*. They may also propose modifications, additions, clarifications, and updates to the *IT Architecture* (including TRM and Standards Profiles). Section 4 of the *FEMA IT Architecture* provides guidelines for requests of waivers, deviations, and exceptions.
- The TRM and Standards Profiles shall apply across the life cycle of an IT system.
- The TRM and Standards Profiles shall be used in major IT systems acquisitions and developments. It is recommended that a technical approach for achieving compliance be part of the evaluation factors.
- The CIO seeks to apply IT standards and standard tools consistently and uniformly throughout the organization.

2.2 FEMA Technical Reference Model (TRM)

2.2.1 Key Architectural Issues Associated with Standards

There are a number of important technical and managerial issues that impact multiple Federal agencies and are currently beyond the control of FEMA. Some of these architectural issues are still unsettled across the IT community and with the National Archives (especially in light of the recent court decision, *Public Citizen v. Carlin*). In general, these issues are contributing to the difficulty that Federal agencies like FEMA have in implementing open, interoperable, and standardized approaches in consensus with their business partners. These unsettled issues contribute, as background factors, to FEMA's status as a consumer, not a developer, of standards and standards profiles. Eight of these issues are stated and discussed in Appendix K .

2.2.2 Identification and Description of Major FEMA IT Services

The major IT services and architectural components are identified and described in Appendix N . Appendix N also identifies the relevant IT standards or standard tools and their status at FEMA, and provides appropriate comments.

Standards for networking services and communications services are separately addressed in Section 3. The requirement for security architecture and security standards is addressed in Section 2.4. Minimum requirements for the FEMA standard workstation (e.g., processor, memory, video display, data storage and I/O media, network ports, energy conservation, monitor, etc.) are stated in the *FEMA Information Resources Management Procedural Directive (FIRMPD)*.

2.3 FEMA Standards Profiles

2.3.1 Nature of a Standards Profile

Because of its relatively small role in the marketplace and in light of the crosscutting issues referred to in Section 2.2.1 and discussed in Appendix K , the FEMA CIO will not develop standards profiles. FEMA may adopt, very selectively, and exploit existing and widely accepted standards profiles in close coordination with FEMA's business partners. As a general practice, FEMA will purchase and use the tools that the Agency finds to offer the best overall advantage.

2.3.2 Identification of Major IT Standards in the FEMA High-Level TRM Framework

Selected standards that offer significant potential for achieving openness across FEMA's IT systems in the future are identified in Appendix O .

2.4 FEMA Security Architecture

At this stage of development of the initial *FEMA IT Architecture*, a detailed Security Architecture has not yet been developed. A robust implementable and comprehensive Security Architecture is recognized to be important for future IT systems development and integration at FEMA, and will be reflected in future revisions to this document.

In developing the FEMA Security Architecture, FEMA is cognizant of the requirement for Critical Infrastructure Protection (CIP) contained in Executive Order 13010 and Presidential Decision Directive 63 (PDD-63). PDD-63 mandates the Federal government to achieve and maintain the ability to protect the critical infrastructure from intentional acts of harm. The critical infrastructure includes the physical and cyber-based systems essential to the operations of the economy and government. FEMA recognizes that close cooperation with State and local governments, and first responders is essential for a robust and flexible infrastructure protection program.

FEMA is responsible for protecting its own critical infrastructure, especially its cyber-based systems. The CIO for FEMA also serves as the agency's Chief Infrastructure Assurance Officer (CIAO). By November 1998, as a matter of high priority, the CIAO will propose a plan for protecting FEMA's critical infrastructure, which shall include vulnerability assessment of IT systems, networks, and physical systems, as well as recommendations for eliminating significant vulnerabilities. It is anticipated that this plan will set the stage for development of a comprehensive FEMA Security Architecture to meet the requirement of the CIP program. The remainder of this section identifies the basic approach and methodology for development of the FEMA Security Architecture, which is under consideration.

The purpose of this section of the FEMA Technical Reference Model is to provide the high-level guidelines and to describe the preferred methodology for future development of the FEMA enterprise-wide Security Architecture.

Accordingly, this section defines a standardized architectural approach for:

1. Identifying required security services for FEMA IT systems and networks
2. Analyzing the security implications and requirements for IT systems and networks
3. Allocating security mechanisms to meet the requirements.

This section of the TRM also provides high-level Security Architecture guidelines for FEMA information system developers as they plan for the hardware and software design implementations. System developers need to determine if security measures that they are implementing in their systems provide sufficient services for authentication, access control, data confidentiality, data integrity, availability, and non-repudiation, or whether additional system-specific security services and mechanisms must be developed.

2.4.1 Preferred Methodology for Development of a Security Architecture

This FEMA TRM adopts the basic concepts described in the following documents as the preferred methodology for development of an enterprise-wide Security Architecture:

1. *Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, Department of Defense Goal Security Architecture (DGSA)*
2. *International Standard, ISO 7498-2, Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.*

The two documents identified above provide proven high-level architecture development concepts that have been widely used throughout government and industry for the development of Security Architectures. The methodology is responsive to the requirements of PDD-63 to address and analyze security of cyber systems and networks.

2.4.2 Goals of the FEMA Security Architecture

One of the major goals of the FEMA Security Architecture will be to define where in the overall information systems architecture that security services need to be provided. The FEMA Security Architecture will also define the mechanisms to provide the required services. As the FEMA IT Architecture evolves and is implemented, the Security Architecture will allow system developers to determine what, if any, enhancements must be made to development programs to meet the security requirements.

Since it is impossible to foresee all future security requirements, the FEMA Security Architecture must be flexible to meet the requirements of both today's FEMA information systems and near-term development programs. Future IT Architecture developments that might impact the security service allocations include widespread implementation of groupware based on emerging approaches like Java, or establishment of Virtual Private Networks (VPNs) with FEMA business partners.

2.4.3 Security Architecture Development Approach

As noted above, the DoD Goal Security Architecture (DGSA) document and International Standard ISO 7498-2, Part 2, *Security Architecture* document provide a recognized methodology for developing a

FEMA Security Architecture. Critical to any Security Architecture development are the required Security Services and the assigned or allocated Security Mechanisms. Each of these is briefly addressed.

2.4.3.1 Security Services

Within the FEMA Security Architecture, security services are the basic functions that must be provided. These fall into six internationally-agreed upon areas. At the current level of development of the *FEMA IT Architecture*, the FEMA Security Architecture needs to consider the following basic security services.

- **Authentication.** These services establish the validity of a claimed identity
- **Access Control.** These services prevent the unauthorized use of a resource, including preventing the use of a resource in an unauthorized manner
- **Data Confidentiality.** These services protect data from unauthorized disclosure
- **Data Integrity.** These services protect the integrity of data and detect any modification, insertion, deletion or replay of any data within the system
- **Availability.** This service assures resources, applications and data can be accessed by users at a predetermined percentage of the time
- **Non-repudiation.** These services provide either proof of origin of data or proof of delivery of data or both. They protect against any attempt by either the sender or the receiver of the data to falsely deny sending or receiving the data
- **Audit Services.** In addition to the six security services, audit services are added to the Security Architecture. Included with the audit services are intrusion detection and audit reduction mechanisms. Audit services are considered a part of Security Management in the ISO standards.

Additional security services may be added in future revision to this document and as a result of the ongoing analysis in response to PDD-63.

2.4.3.2 Security Mechanisms

Security Mechanisms are defined as administrative measures, physical controls, and hardware and software functions that can be configured and allocated to satisfy the required security services. In the interest of open systems development, FEMA anticipates that the Security Architecture will define the functions that will be provided, and not necessarily the actual hardware and software. For example, the Security Architecture may call for a distributed directory structure without specifying which directory system (UNIX, Windows NT, etc.) will be used. These functions can be thought of as the actual high-level engineering design solutions to provide the required services. This *FEMA IT Architecture* anticipates that in many instances more than one mechanism could be used to provide a required security service.

2.4.4 Security Architecture Methodology

As noted above, both the DGSA and ISO 7498-2 will be used to guide the development of the FEMA Security Architecture. ISO 7498-2 primarily establishes the service definitions. The DGSA provides a good high-level methodology for development of Security Architectures. Consistent with the DGSA approach, Figure 2-2 provides the high-level framework that will be used for developing and characterizing the FEMA Security Architecture.

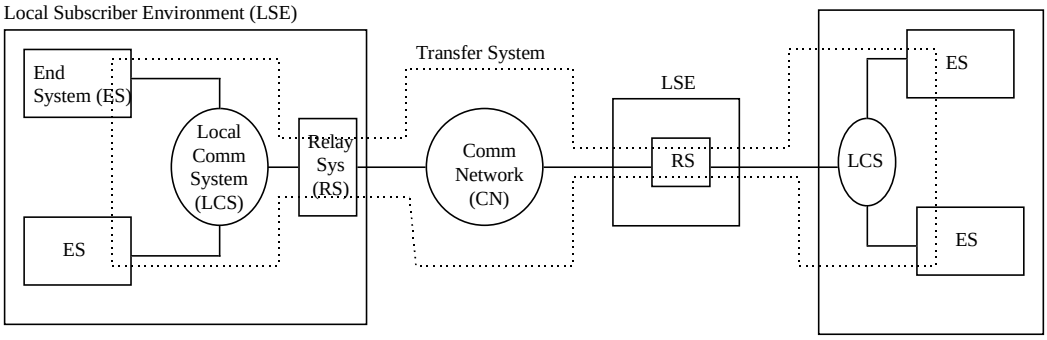

Figure 2-2. Generic Systems and Network Representation Approach to Develop the Security Architecture

As illustrated above, the major Security Architecture elements to be considered include:

- **Local Subscriber Environment (LSE).** The Local Subscriber Environment will include the devices and communications systems under user control. An LSE may contain a single end-user system, such as a workstation, a single relay system such as a router, or a complex interconnection of end systems and relay systems connected through local communications systems. Prime examples of LSEs are computer rooms (such as FEMA command centers, DFOs, and end-user office environments).
- **End System (ES).** End systems consist of a single element, such as a workstation, server, or mainframe. These systems are the basic building blocks of the architecture that provide the data storage and data processing functions.
- **Local Communications System (LCS).** The local communications system consists of the networks within an LSE that supports connection of end systems and provides the interface to relay systems. These are the local area networks (LANs).
- **Relay System (RS).** Consists of communications devices such as multiplexers, routers, switches, cellular nodes, network firewalls, and message transfer agents. The Relay Systems usually provide the interfaces to LSEs and CNs within the *IT Architecture*.
- **Communications Network (CN).** The Communications Network defines the communications network connecting the LSEs and may be communications networks entirely under control of FEMA, such as the FEMA Switched Network or may be public communications entities such as the Internet or other leased networks.
- **Transfer Systems (TS).** Transfer systems can be viewed as the end-to-end application subsystems that make up FEMA's information systems. The Transfer System might typically be composed of a NEMIS user workstation, the FSN backbone, a server or mainframe located in FEMA HQ, and applications that reside on the individual end systems.

3 Communications and Networking

3.1 Overview

This section emphasizes the ***future*** network architecture. To provide a point of reference, the existing FEMA network configuration is described at a high-level. More detailed configuration information for the current network can be obtained from the FEMA National Network Operations Branch (NNOB).

The most significant planned change to the network architecture is the integration of the voice and data networks. This integration will provide performance and cost savings opportunities and will position FEMA to support future technologies, applications, and requirements (such as high bandwidth, integrated voice and video, and data applications). Other important network services are under consideration in the target network architecture. The implementation strategy describes a phased approach that includes prototypes, legacy support, and an event-driven milestone schedule.

3.1.1 Network Architecture Components

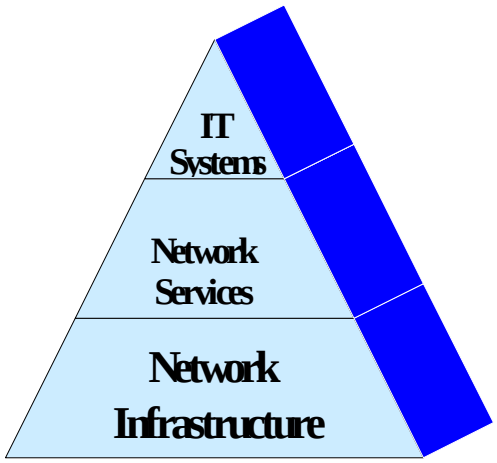

Figure 3-1. Network Architecture Model

As shown in Figure 3-1, the FEMA network architecture model consists of three major layers or components: Network Infrastructure, Network Services, and IT Systems. The network infrastructure is the foundation for the higher layers. The network services component provides a variety of services and supports IT systems and other user elements.

3.1.2 Network Infrastructure

The network infrastructure consists of several elements: transmission, switching systems, and network equipment. Of these, transmission is a significant recurring cost driver. Transmission is

composed of backbone connections (mostly wide-area) and access tail-circuits (mostly local-area). Satellite transmission and reception facilities are also important parts of this component. Switching systems consist of voice switches (PBX), data switches, routers, digital cross-connect switches, and multiplexers. These elements appear in both the wide-area and local-area portions of the network.

3.1.3 Network Services

Network services include voice, video, data, and help desk services. Network services also include important internal functions such as network management and security. Network services may also include services such as virtual private networks (VPNs) and multimedia services (in the future).

3.1.4 IT Systems

IT Systems include user elements and enterprise systems such as the National Emergency Management Information System (NEMIS). IT Systems also include support of unique regional and field requirements and systems such as servers, virtual LANs, and network addressing. Other potential services include Personal Communications Services (PCS), mobile services, bandwidth on-demand, Quality of Service, and security. In addition, the network may need to support enterprise-wide IT services such as (in the future) correspondence and action tracking, text search, digital signature, collaboration and visualization services, interactive GIS, digital library services, etc.

3.1.5 Network Architecture Process

In developing the FEMA network architecture, the ITS Directorate reviewed existing documentation, evaluated vendor products, and interviewed key personnel. This effort included the following major activities:

- Understand FEMA mission and networking requirements, define baseline
    - Study network documentation and diagrams
    - Interview key operations and engineering personnel, tour facilities and equipment.

- Assess network infrastructure for each type of service
    - Circuit and node utilization analysis
    - Network management, problem detection, and diagnosis
    - Deficiencies, points of failure
    - Maintenance emphasis and issues
    - Growth patterns and projections.

- Identify alternatives, enhancements, upgrades, and new technology
    - Vendor product evaluations
    - Integration of voice, video, data, and network management
    - Support of ITA recommendations (new functions and technologies).

- Recommend evolutionary approach

- Proof-of-concept demonstrations
- No downtime, phased integration, hybrid approach
- Transition milestones based on needs and events.
  - Capacity, cost/benefit
  - Performance, availability
  - Training and readiness.

3.2 Existing Network Architecture

This section provides a high-level overview of the existing FEMA network architecture. The primary purpose is to provide a baseline and context for the discussion of architecture requirements and alternatives presented in later sections.

The existing network architecture is a snapshot taken during the ITA and NTA development process. Since it is only a snapshot, up-to-date configuration information needs to be obtained to assess the full cost and impact of changes to FEMA networks. As shown in Figure 3-2, the NNOB is a part of the Operations Division and maintains current configuration information for FEMA communications networks.

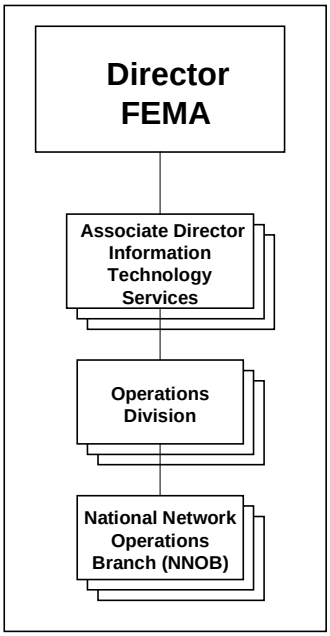

Figure 3-2. National Network Operations Branch (NNOB)

The following sections describe the existing network architecture in three major subsections: Network Infrastructure, Network Services, and IT Systems and User Elements.

3.2.1 Network Infrastructure

FEMA has two primary networks: a switched network and a data network. An overlapping network of point-to-point and switched connections provides the transmission infrastructure for both networks.

Within FEMA, the term *FEMA Switched Network*, or FSN, generally refers to the entire enterprise of voice, data, and supporting networks. Figure 3-3 illustrates the enterprise network, which is divided into Regions, States, and other territories.

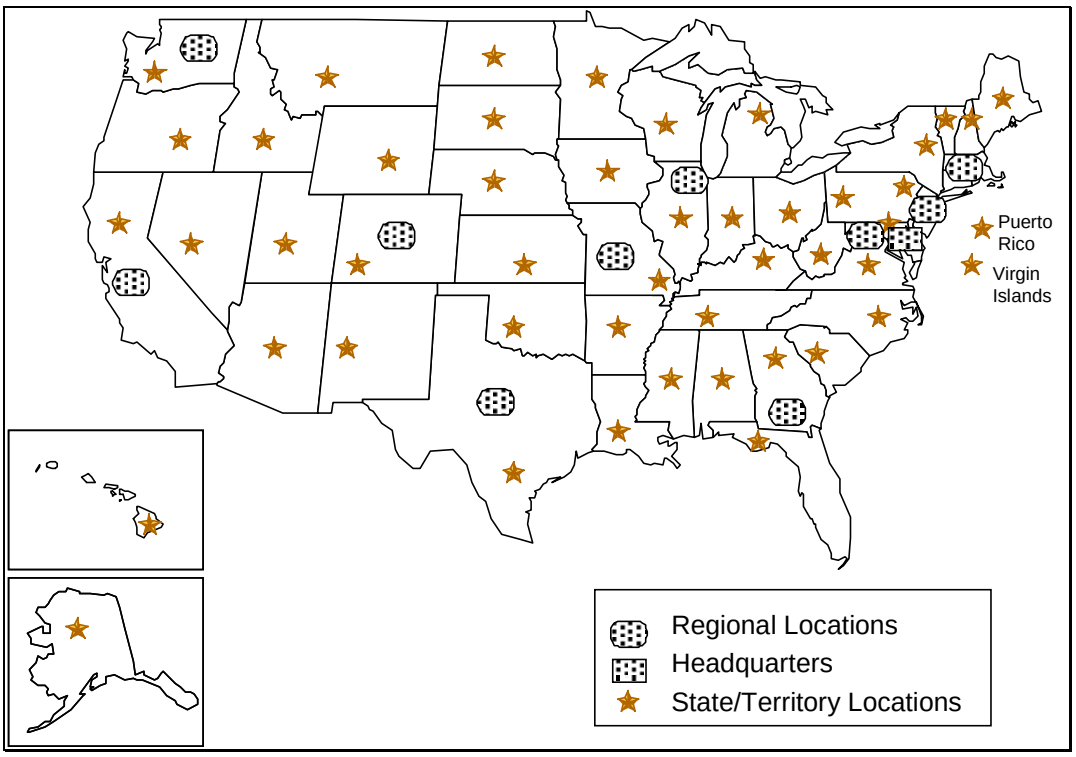

Figure 3-3. FEMA Enterprise Network

FEMA personnel also frequently use the term FSN in reference only to the voice network. For purposes of this document, the meaning of the term FSN will be more clearly stated. The terms *voice network* or *switched network* are used to refer to the PBX network, which primarily provides voice services to FEMA. The term *data network* refers to the router network, which primarily provides data services.

3.2.1.1 Switched Network

The primary function of the switched network is to transport FEMA voice communications. A network of PBXs and multiplexers is used to provide a variety of voice and dial-up services. The switched network also provides external connections via the Public Switched Network (PSN) and the Federal Telecommunications System (FTS). In addition, the switched network can transport data and video connections via the integrated multiplexers. The PBX switching architecture is shown in Figure 3-4.

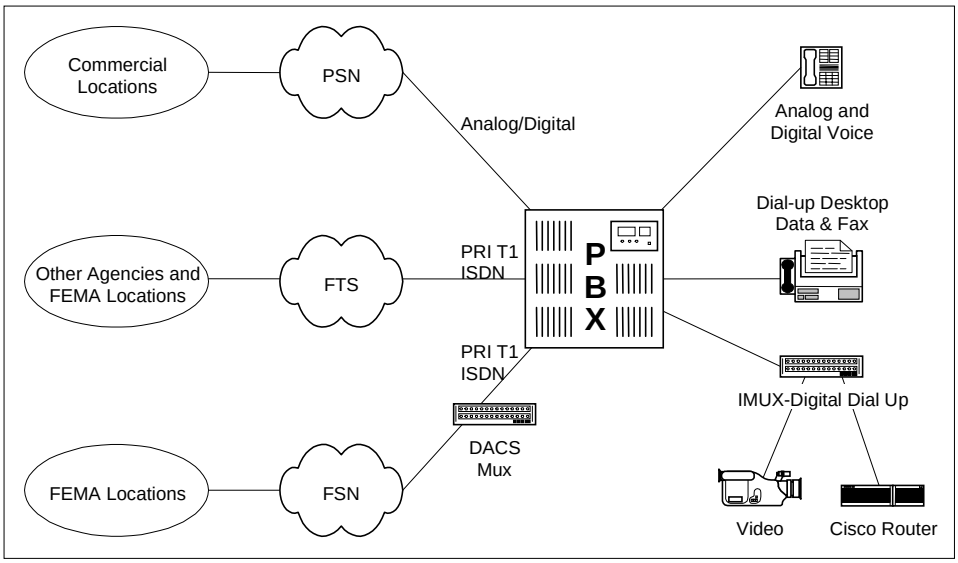

Figure 3-4. Switched Network Configuration

The primary nodes of the current switched network are interconnected in a hierarchical configuration. Mt. Weather, VA; Denver, CO; and Denton TX are at the top of the hierarchy. Dedicated connections to the Disaster Field Offices (DFO) are provided from Mt. Weather.

The PBX switches are programmed to route calls in the most cost-effective manner. The first priority is to route calls over the dedicated switched network (FSN). If the location is not reachable for any reason, the next choice path is FTS followed by the PSN. Figure 3-5 illustrates the connectivity of the primary nodes and locations in the switched network.

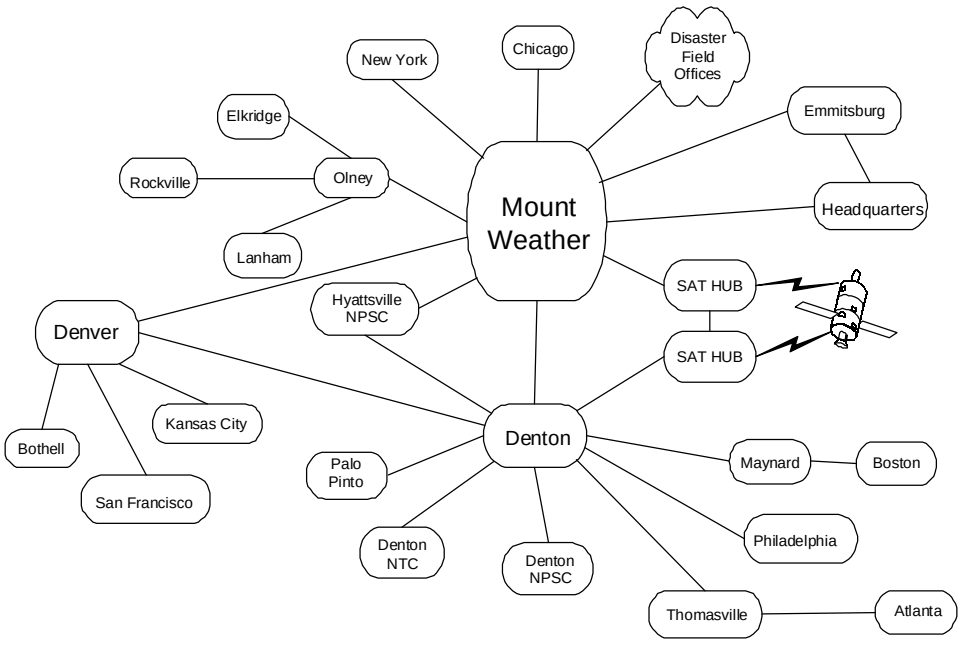

Figure 3-5. Switched Network Connectivity

3.2.1.2 Data Network

The primary function of the current data network is to transport FEMA data traffic over the FEMA Intranet. The data network also has connections to the public Internet via firewalls. As shown in Figure 3-6, a network of routers are currently used to extend FEMA data services across the country and to other territories. The connectivity between routers is provided primarily by dedicated T1 circuits. Some connectivity is provided over the switched network using dial-up connections and multiplexers.

At each FEMA location, the routers provide connectivity for enterprise servers, LAN segments, and other clients. Switches and hubs distribute the connectivity to the LAN segments. The network contains approximately 80 routers and 94 Ethernet switches.

Two types of routing protocols are currently run on FEMA routers. Cisco's proprietary Interior Gateway Routing Protocol (IGRP) is used to route Internet Protocol (IP) traffic and Routing Information Protocol (RIP) is used to route Novell Internetwork Packet Exchange (IPX) traffic. IP address segments are provided from a single class B address. In the future, FEMA may transition to a single consolidated routing protocol.

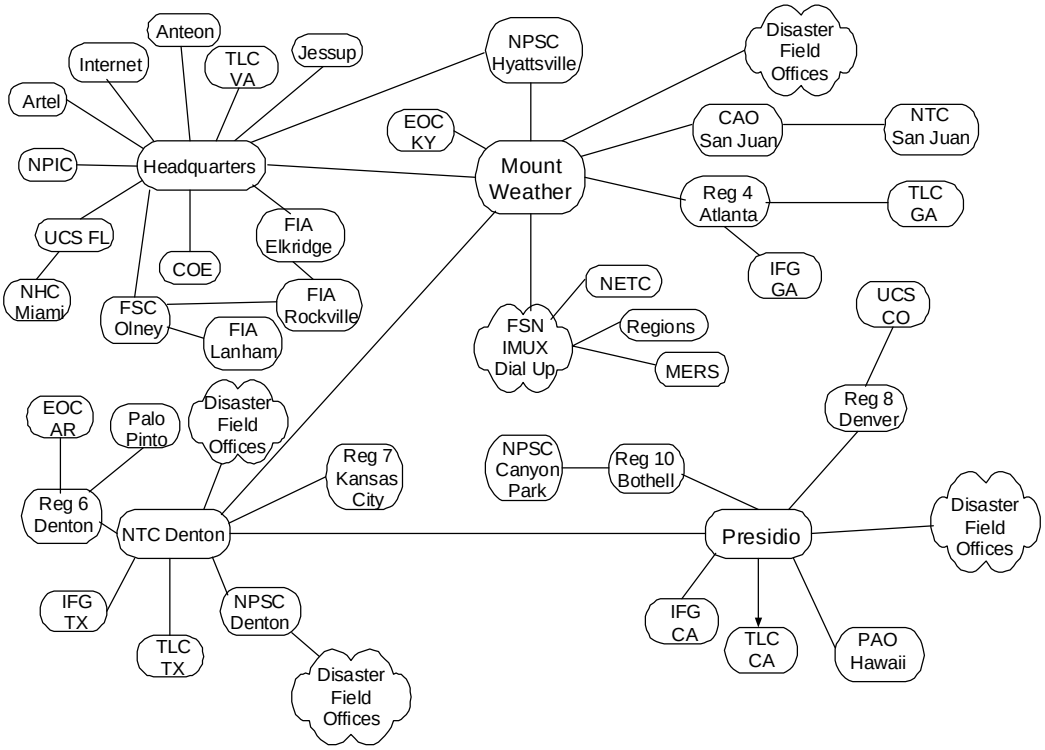

Figure 3-6. Data Network Connectivity

3.2.1.3 Transmission

In the current network architecture, the primary transmission medium is the ISDN PRI T1. Both the switched network and the data network rely heavily on T1 transmission. Satellite

transmission (T1) is used to quickly establish connectivity in disaster areas. The satellite connection is replaced by traditional T1 circuits when the local infrastructure can support it.

Due to the separate origins of the data network and the voice network, there are separate voice (switched) and data T1 circuits to most FEMA locations. Table 3-1 is a summary of the current T1 circuits and monthly recurring costs.

Table 3-1. T1 Summary

Network	Quantity of T1 circuits	Monthly Recurring Cost
Data	**47**	**$157,127.00**
Switched (Voice)	**39**	**$94,955.56**
Total	**86**	**$252,082.56**

3.2.1.4 Network Equipment

The National Network Operations Center (NNOC) at Mount Weather currently maintains centralized control and management of network equipment. Table 3-2 summarizes the major types of network equipment. The quantity of equipment listed in the table is nominal and changes over time due to disaster support and routine maintenance. These quantities do not include the communications equipment in the Mobile Emergency Response System (MERS) and Mobile And Transportable Telecommunications System (MATTS).

Table 3-2. Major Network Equipment Types

Network Equipment Type	Description
PBX	Private Branch Exchange switches. Quantities: 5 Merlin, 2 Meridian SL1, 9 System 85, 20 G3, 2 G2.
Multiplexers	Aggregate communications channels for transport over switched network. Quantities: 32 Inverse Multiplexers, 80 DACS and subrate multiplexers, 15 IDNX multiplexers.
Routers	Cisco routers for data network. Quantities: 90.
Voice Messaging	Quantities: 11 Audix.

3.2.2 Network Services

FEMA provides a number of network services including the following:

- Voice, video, data
- E-mail, messaging
- Local and wide area connectivity

- Ordering and billing
- Cellular phones and pagers
- Point-to-point and dial-up circuits
- Facsimile
- Desktop services
- Security (physical and logical)
- Bandwidth management
- Network and systems management
- Configuration management
- Help desk, trouble reports.

Two of the services, *Network and systems management* and *Security*, are discussed in more detail below.

3.2.2.1 Network and Systems Management Tools

Several network services and equipment require special tools and expertise. Table 3-3 lists standard tools currently used to provide network and systems management services.

Table 3-3. Standard Tools Used for Network and Systems Management

Service Category	Software Product Name	Description
Network Management	HP OpenView	Provides platform for network management applications.
Network Management	CWSI	Cisco Works for Switched Internets. Manage Cisco switching platforms.
Network Management	CiscoWorks	Detailed management of all Cisco routers.
Network Management	NetSys	Network debugging tools for managing, tuning, and planning growth of FEMA networks.
Network Management	RCS	Routing control system for changing configuration of 800 call routes.
Network Management	CMS	Call Management System. Four locations to do agent traffic analysis.
Network Management	Comsphere 6800	Manage TDM multiplexers including 745 DACS Mux and 740 Channel Mux.
Network Management	ProCom	No Network Management System for IMUX. Use PC with ProCom to dial-up IMUX.
Network Management	NetOpen 5000	Manage IDNX.
Network Management	G3-MA	Manage G3 PBX.
Network Management	Monitor 1	Traffic statistics and analysis (PBX).
Systems Management	SPM	Tool to configure Merlin. System Programming and Maintenance (SPM) software that allows System Administrator to program system features and make moves and changes.

Service Category	Software Product Name	Description
Systems Management	Remedy Trouble Ticketing	Used by the NOC to create and track network and system failures and errors. These are created by help desk support personnel or NOC technicians.
Systems Management	Voice Management System	Tool to manage PBX. At each site with PBX.
Systems Management	Manager 4	Tool to administratively manage System 85 and G2.
Systems Management	Accumaster Trouble Tracker	Used by the NOC to create and track network and system failures and errors for the Lucent voice components.
Systems Management	Accugraph	Provides physical Configuration Management.

3.2.2.2 Network Security

Network security is an important requirement for FEMA networks. Currently, FEMA data networks are protected with physical and logical security measures. The networks provide limited points of access and highly restrictive firewalls. All new products and technologies must be carefully evaluated for security risks. Network security will be addressed in more detail as part of the planned Security Architecture mentioned in Section 2.4 and in response to PDD-63 on Critical Infrastructure Protection.

3.2.3 IT Systems and User Elements

As mentioned in the previous section, several types of services are necessary to operate and maintain the network. At a higher level of the functional hierarchy, enterprise-wide information systems also need to be provided and supported. The most significant FEMA IT system currently being fielded is NEMIS. Other IT systems requiring care and attention in the existing networks are discussed in Sections 1 and 4 of this document.

3.3 Requirements and Opportunities

The assessments and recommendations in this section are based on analysis of FEMA documentation and a series of discussions among FEMA engineering and operations personnel.

Overall, existing FEMA networks currently satisfy all mission-critical requirements. Sufficient bandwidth exists in both the voice network and the data network. Separate network management systems and tools and experienced staff provide FEMA with a responsive network management capability. With current systems, FEMA engineers and technicians can quickly install and troubleshoot network components in emergency situations and adverse environments.

While the current network architecture functions well, the performance and cost effectiveness of FEMA networks can be significantly improved. New network technologies can also expand and improve the current network services. The following paragraphs and later sections discuss potential requirements, opportunities, alternatives, and architecture recommendations.

3.3.1 Integration of Backbone Transmission

As previously described, FEMA effectively operates and maintains two distinct networks. Each network is essentially supported by separate transmission networks. There is some sharing of transmission via multiplexers and dial-up circuits, but the majority of transmission bandwidth is not shared. Significant savings in equipment and recurring costs can be realized if both types of network traffic can be shared over a single transmission network.

3.3.2 Voice over Data Networks

Voice over data networks, such as IP, is a technology that potentially offers unique cost savings and new capabilities. Costs can be reduced by shifting some of the voice traffic to the data network where bandwidth is more effectively shared. Costs could also be reduced by reducing the amount of equipment required at some locations, particularly disaster areas.

Voice over data networks offers other advantages particularly to disaster areas. For example, in deployments to disaster areas, separate T1 circuits are currently ordered for voice and data communications. Due to regulatory differences, the data circuits can be expedited and installed prior to the voice circuits. With voice over data networks, voice service could be established at the same time as the data service.

The investigation of voice over data networks needs to address Quality of Service, gateways between the data and voice networks, reliability, etc. A related capability that is under consideration as a potential network architectural component is Computer Telephony Integration or CTI. The value of integrating common desktop functions needs to be evaluated against the cost of implementation and support.

3.3.3 Integrated Network and Configuration Management

While current network management systems operate effectively, there is a significant opportunity to automate and simplify. As shown in Table 3-3, numerous systems and tools are currently required to manage and monitor the networks. In addition, an around-the-clock staff of cross-trained technicians is required to attend each system. Potential architectural improvements under consideration include provision of tools that would provide automated discovery of network configuration changes and correlation of alarms. The integrated presentation of network performance, problems, and configuration information is also being investigated.

3.3.4 IP Address Management

Related to the issues of network management is the issue of IP address management. Current IP management is essentially a manual process. While this process works effectively today, there is generally a need to implement methods that can increase mobility, reconfiguration time, and manageability.

3.3.5 Derived ITA Network Requirements

In developing this initial *IT Architecture* document, FEMA identified a number of potentially important operational factors that impact the target network architecture.

3.3.5.1 Multicasting

The broadcast or multicast of information to disaster areas and supporting organizations is an important capability that must be supported by the target network architecture. For example, within FEMA, Emergency Information and Media Affairs currently broadcasts multimedia to disaster areas using a proprietary methodology. Due to network and application limitations, the number of simultaneous connections is limited to 60. However, in the event of a large disaster, it will be necessary to disseminate information to a much wider audience, on the order of tens of thousands or greater.

3.3.5.2 Extranets and Virtual Private Networks

ITA discussions with the FEMA Regions indicated a need for better networking to State and local governments and other regional assets. Since FEMA security policies and firewalls restrict external access, a better method of communicating within Regions is required. The Regions specifically expressed a desire to evaluate and prototype Extranets and Virtual Private Networks (VPNs) to provide increased flexibility, bandwidth, and control within Regions. As stated previously, security issues need to be evaluated to ensure that the integrity of existing networks is not degraded. Similarly, network management systems and policies may need to be enhanced (or decentralized) to maintain smooth operations and support. These requirements are now under consideration for potential impact on the network architecture.

3.3.5.3 High Bandwidth

The projected need for more bandwidth is a commonly stated requirement among FEMA organizations. As an example, the Mitigation Directorate estimates that GIS archives may reach petabytes (1,000 terabytes) to support mitigation in the future. While the network will only need to transport a small fraction of the GIS information at any given instant, the bandwidth required may still be extensive. This situation is particularly true if the need is for interactive access to GIS archives and the amount of GIS information to be retrieved in any interactive query is large (e.g., greater than megabytes).

3.3.5.4 Modeling and Simulation Support

The U.S. Fire Administration has indicated a desire to evaluate advanced modeling and simulation applications such as 3D virtual reality. Virtual reality applications will allow realistic simulations of search and rescue (SAR) scenarios or arson scenes so that fire marshals might inspect evidence and safely experience the crime scene for training purposes. This potential requirement implies a need for the target network architecture to be scalable and provide high performance in a number of areas, including bandwidth and latency. Local- versus wide-area requirements will also need to be evaluated and refined to ensure the network can provide the required services at an affordable cost.

3.3.5.5 Exercise Training and Analysis

Another ITA-derived requirement that the future network will need to support is exercise training and analysis. This requirement includes support for computer-based training, online exercises, classroom instruction, and similar multimedia requirements. The PT&E Directorate is one of the FEMA organizations that needs a properly designed network to support these requirements. Necessary network characteristics include scalable bandwidth and low delays (e.g., latency).

3.4 Target Network Architecture

3.4.1 Overview

This section identifies and discusses important characteristics and objectives of a candidate target network architecture that satisfies current and future FEMA requirements. Specific technologies and product types to evaluate are suggested and are under active evaluation within FEMA. The suggestions are based on evaluations of requirements and opportunities, and on the current or near-term availability of mature products and technologies.

3.4.2 Objectives and Criteria

As previously stated, existing FEMA networks work well and satisfy all current mission-critical requirements. Therefore, it is important that any modifications to the current architecture offer significant advantages, cost savings, or new capabilities. The following paragraphs summarize some of the key objectives and criteria that the FEMA ITS Directorate are considering.

3.4.2.1 Cost Effectiveness

The target architecture should provide an early return on investment in terms of lower recurring costs and reduced infrastructure support costs. This potential return can be accomplished, for example, with a reduction in the number of point-to-point T1 circuits required for the backbone voice and data networks. Further infrastructure and support savings could be achieved by integrating voice and data functions in a single platform.

3.4.2.2 Simplicity and Manageability

Complex systems and technologies are difficult to operate and maintain. In contrast, well-designed systems and products are usually easier to integrate and manage. Hands-on product evaluations and working prototypes are some of the best methods of evaluating these criteria.

3.4.2.3 Reliability, Availability, Survivability, and Maintainability

High reliability, availability, survivability, and maintainability are important characteristics of equipment, networks and supporting systems. Network integration poses additional issues because voice networks and data networks have traditionally not been held to the same standards. Therefore, it is important to ensure that the target architecture does not degrade the performance of existing networks. FEMA recognizes that it is equally important to engineer affordable systems-level requirements and not arbitrarily impose 99.999 criteria on all aspects of the target architecture.

3.4.2.4 Low Risk, Minimum Downtime

Risk is inherent in any technology upgrade. FEMA engineers are satisfied that the network engineering risk in migrating to a target architecture can be identified and managed. Likewise, equipment and implementation strategies can be designed to minimize downtime during network upgrades and integration.

3.4.2.5 Security

As previously stated, FEMA maintains the security of the voice and data networks by using point-to-point connections, private infrastructure, and firewalls. In addition, the networks are continually monitored and evaluated for security risks.

At the current level of target network architecture development, FEMA has not yet evaluated all the security issues associated with new products and technologies. For example, varieties of security options are possible when using Virtual Private Networks (VPN). Similarly, ATM provides virtual circuit connectivity analogous to physical point-to-point circuits. FEMA will evaluate the architecture and specific security issues well prior to implementation.

The methodology for addressing the security aspects of the target architecture is outlined in Section 2.4 and will be responsive to the requirements of the Critical Infrastructure Protection (CIP) program.

3.4.2.6 Product Maturity

FEMA recognizes that alternative products should also be evaluated in terms of product maturity. FEMA cannot afford to utilize developmental or beta equipment in the operational networks. Representative indicators of product maturity that will be considered will include *years on the market* and *market share*.

3.4.2.7 Standards, Interoperability, and Legacy Support

Where clear choices are available, FEMA intends to select standards-based products over proprietary products and implementations. The products will be thoroughly tested to ensure interoperability and support of legacy systems. The use of standards will provide more flexibility, increase leverage, and broaden the range of product alternatives.

3.4.2.8 Performance

As a requirement, the target architecture must perform better than or equal to existing capabilities. In addition to standard network performance requirements such as high network availability, new technologies are expected to offer performance-enhancing characteristics as outlined below:

- More efficient bandwidth utilization
- Better dynamic bandwidth allocation
- Bandwidth-on-demand
- Better fault tolerance and recovery
- Graceful degradation.

3.4.2.9 Quality of Service (QoS)

In the design of the target network architecture, FEMA recognizes that Quality of Service (QoS) is extremely important for the success of integrated networks. QoS must be manageable and measurable. FEMA will address QoS factors at several architecture levels including:

- Transmission-level: Circuits and trunks, Bit error, Delay, etc.
- Application-level: Voice, Data, Video, NEMIS, Messaging, etc.
- System-level: Manageability, Supportability, Security, etc.

3.4.3 Evaluation of Alternative Backbone Transport Protocols

FEMA recognizes that several different communications technologies alternatives could be used to integrate the backbones of FEMA voice and data networks (OSI Layer 3 and below). This section outlines some common technologies and alternatives that were considered as candidates for the target network architecture. The last alternative, Asynchronous Transfer Mode (ATM), is currently being evaluated for use in a future integrated backbone network.

3.4.3.1 Synchronous Optical Network (SONET)

SONET is a high speed switching and multiplexing technology. SONET backbones are often used to provide highly reliable transport. SONET offers transmission and self-healing features that are required by telecommunications carriers and large agencies with similar requirements.

A SONET backbone could be used to transport FEMA voice, video, and data traffic. The high-speed, self-healing characteristics of SONET would help increase the robustness of FEMA networks.

Despite the advantages, a SONET backbone is not currently recommended for several reasons. First, FEMA bandwidth requirements are on the low end compared to typical SONET backbone requirements. Second, current switching and routing systems now have characteristics similar to SONET including high availability and the ability to quickly route around failures. Finally, other technologies, like ATM, can perform similar functions with better efficiency due to statistical multiplexing.

3.4.3.2 Frame Relay

Frame Relay is another alternative for data communications. Although Frame Relay is also one of the technologies used to transport voice communications, Frame Relay is not preferred in the FEMA target architecture for two primary reasons. First, scalability is an issue since Frame Relay is typically employed for low-speed links (T1 and below). Secondly, Frame Relay is not the best choice to provide all the required characteristics of an integrating technology in one protocol. For the future, ITA applications that have been suggested will require characteristics that include high speed, low latency, low delay variation, efficient statistical multiplexing, and a mature QoS. In order to meet all these requirements, even Frame Relay needs to be transported over ATM, adding additional overhead.

3.4.3.3 Internet Protocol (IP)

IP is also not preferred as the common transport protocol for the integrated backbone network. The rationale is similar to Frame Relay in the previous section. IP was not designed to deliver the precise QoS required for integrated backbone transmission of voice and data communications. The Internet Engineering Task Force (IETF) and router vendors are working to improve and standardize QoS over IP. In the future, IP may become a more viable transport protocol for integrated voice, video, and data applications. Note that while IP is not recommended for common backbone transport, multimedia applications (like voice over IP) will continue to proliferate and increase the need for a high performance backbone with QoS.

3.4.3.4 Asynchronous Transfer Mode (ATM)

ATM is the only statistical multiplexing protocol specifically designed to integrate the demanding requirements of voice, video, and data traffic streams in a scaleable manner. ATM addresses several technical issues involved with the integration of multimedia traffic over a common backbone. Most importantly, ATM has mature QoS and traffic management features. Each traffic stream can have a unique set of requirements including bandwidth, delay, jitter, error rate, etc.

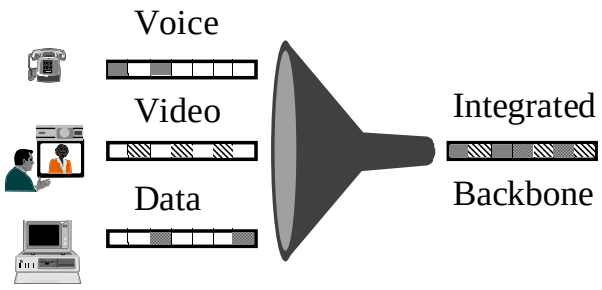

Figure 3-7. Asynchronous Transfer Mode (ATM)

ATM is attractive to FEMA because it can be easily implemented over dedicated point-to-point links or over more cost-effective leased commercial services. The statistical multiplexing nature of ATM allows multiple types of communications streams to share the same or separate physical connections. Virtual circuits or channels provide pathways for the streams and advanced QoS mechanisms ensure the streams get the bandwidth and quality required. The potential for ATM to support virtual circuits and Virtual Private Networks is of interest to FEMA Regions since it affords future opportunities to establish secure scaleable connectivity with States and local governments.

3.4.4 Target Network Architecture Recommendations

The overarching theme of the FEMA target network architecture is *integration*. Corporations, carriers, and government agencies have started integrating their networks at the backbone level and at the services level. FEMA networks can also be integrated, however, integration must be properly designed and accomplished carefully.

The following sections identify new technologies and services that are under active consideration for integration into the FEMA network architecture. Section 3.5 provides a candidate network transition strategy that is under development at FEMA.

3.4.4.1 Network Architecture

The target network architecture is explained in terms of the two major components:
1) Transmission and 2) Switching and routing.

Transmission - FEMA has a mix of transmission media that include point-to-point, switched services, dial-up, SATCOM and other wireless media.

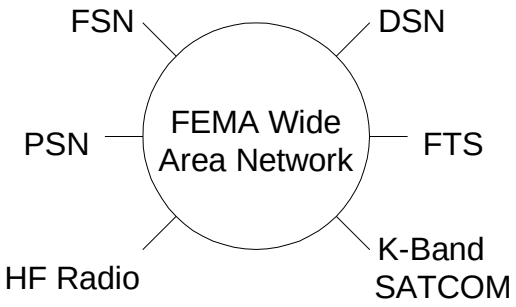

Figure 3-8. FEMA Transmission Media

The primary recommendation for the target architecture is to integrate the separate voice/data transmission circuits. Instead of traditional TDM methods, the preferred transmission protocol is ATM.

With technologies such as ATM, FEMA can significantly reduce the number of transmission links in the backbone and to the field locations, perhaps by a factor of two. The savings in recurring costs can be expected to quickly pay for the initial investment. A detailed network and cost analysis is needed to accurately size the network connections and to determine the new cost structure.

In the target network architecture, FEMA will be able to use QoS features to manage specific connections and types of service. QoS features will be particularly important for voice and other time sensitive traffic. QoS management will be an evaluation criterion in the selection of vendors and products.

In the target network architecture, the protocols and switching equipment must be able to scale to handle all current and projected FEMA requirements. Scalability is important not just for future growth, but also for handling timing-sensitive applications like voice, video and simulations. As illustrated in Figure 3-9, the target architecture must be able to scale to handle a variety of applications that have been suggested by various FEMA organizations during the development of this initial *FEMA IT Architecture* document. The target architecture must also provide the infrastructure necessary to efficiently support the ITA-derived requirements discussed in Section 3.3.5, including multicasting and virtual networks.

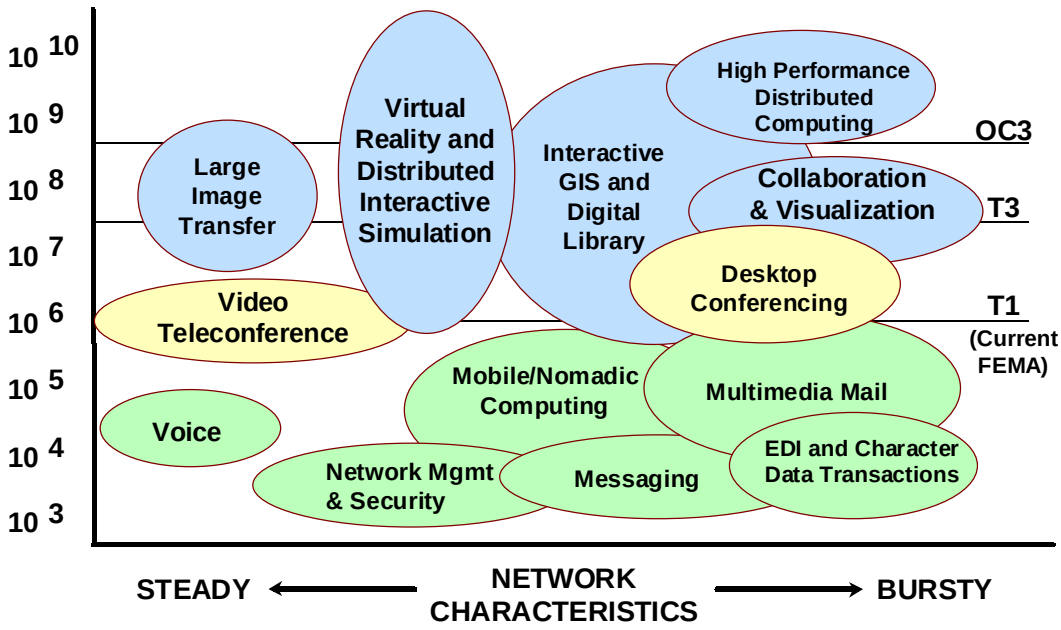

Figure 3-9. Importance of Protocol Scalability

Switching and Routing - The integration and convergence of voice, video, and data services recommended at the transmission layer is also recommended for inclusion in the target network architecture at the switching and routing layer. Multi-function systems now offer bridging, routing, switching, multiplexing services in one platform. The potential advantages of single platform systems include the following:

- Reduced equipment counts
- Reduced training time and maintenance costs
- Faster and easier setup time
- Integrated network management.

Potential disadvantages that will need to be mitigated in the network systems engineering and integration process include:

- Single point of failure
- Less interface options
- Less specialization
- Single vendor.

The single point of failure issue can be mitigated with optional redundant power supplies, hot swappable modules, redundant processor units, etc. Nevertheless, more types of traffic are being concentrated on fewer platforms, which increases the importance of availability specifications. The single vendor issue will be evaluated in the context of performance, cost, service, interoperability and other factors that influence a decision.

If ATM is implemented as the common backbone protocol, other changes in the data routing and switching layers will also be evaluated. In particular, there will be an opportunity to maximize switching and minimize routing. Where routing is necessary, one-arm router configurations can be used instead of traditional multi-arm ("milking machine") routers. This configuration will

maximize the speed of the network and reduce the number of router hops and the number of routers necessary in the network. While router performance is always improving, FEMA expects that switches will probably retain cost/performance advantages due to the hardware and software architecture of the devices.

To further enhance the performance of the (data) network, a single layer 3 protocol and a single routing protocol such as Open Shortest Path First (OSPF) will be considered for incorporation into the network architecture. IP is the *de facto* Internet standard. FEMA anticipates that other protocols, such as IPX, can gradually be phased out in favor of IP. Today, RIP and IGRP are the routing protocols run on all FEMA routers. The transition to a single routing protocol will make routing more efficient and will simplify router maintenance. OSPF is recommended over the existing protocols because it is non-proprietary. OSPF also scales well and is the basis for similar protocols, such as the ATM routing protocol (PNNI).

3.4.4.2 Network Services

In response to the *IT Architecture* requirements, additional network services are being considered for incorporation in the target network architecture. Note that existing legacy network services are assumed to remain a part of the target architecture.

- **Virtual Private Networks (VPN)** - Virtual Private Networks offer the potential to increase the reach and flexibility of FEMA networks. Significant cost reductions are also possible. The VPN technology can be IP, Frame Relay, or ATM. An important issue with VPNs is security, since VPNs extend private networks over other private and public networks.

  Varieties of VPN security options are possible and are under active consideration. A VPN can be created by tunneling through the public Internet using payload encryption. Alternatively, Internet Service Providers (ISP) can setup a protected network that does not traverse the public side of routers.

  The VPN options need to be supported by appropriate QoS and Service Level Agreements. QoS and SLA provisions need to be independently verified to ensure all service requirements are met. Independent verification is required whether the service technology is ATM, IP or another technology. In general, the requirements for specifying QoS in FEMA procurements will also need to be developed and understood by FEMA procurement specialists. The Information Resources Board and the ITS Directorate appreciate the need to develop and specify new contractual vehicles to acquire a new service (such as ATM).

- **Enhanced Firewalls** - A flexible firewall with high-speed Internet access is recommended for FEMA. Today FEMA essentially blocks all incoming traffic from the Internet. While this approach is one of the safest firewall alternatives, it may be overly restrictive because the Internet is a cost-effective means of extending the network. The speed of the firewall is also an important consideration as Internet access requirements grow. Security concerns will need to be evaluated to determine the type and configuration of firewalls permitted in the target network architecture.

- **Personal Communications Services (PCS)** - Another technology and service that is being investigated and can be integrated with existing FEMA networks is Personal Communication Services or PCS. PCS offers mobile users the potential of

integrating wireless communications, messaging, data, and other useful features. As indicated in *IT Architecture* interviews with the Regions, PCS technology can be extremely valuable in disaster areas, and can also be employed by other mobile users. PCS technology can also be integrated with data services and multimedia services to extend the reach and value of the network (e.g., distance learning).

- **Universal Messaging and Directory Services** - Messaging is a valuable service provided by the voice and data networks. With a universal messaging system, fixed and mobile users can more easily manage their time and resources. Similarly, a universal directory service makes it easier to locate and contact personnel and other resources. FEMA is currently assessing the requirements for messaging and directory services, and the extent to which messaging and directory services can and should be integrated with other services such as paging, PCS, and multimedia services.

- **Support for Thin-Client Networks.** A thin-client approach using technology such as Windows Terminal Server, Oracle Network Computing Architecture, and potentially Java applets presents some interesting opportunities for future systems engineering and integration in a distributed field environment. The fact that FEMA has a number of computers with the Emergency Support Teams and at the Disaster Field Offices that have to be set up quickly, with short-term users, and managed in difficult environments argues for a closer look at this technology.

- **Multimedia Services** – As indicated in *IT Architecture* discussions across FEMA Directorates, FEMA must plan to support the trend to mixed and multimedia services, networks, and applications. The benefits of enhanced multimedia services include alternate communication channels, visual feedback, distance learning, reduced necessity for on-site travel, etc. As noted previously, FEMA can establish data circuits sooner than voice circuits; thus making multimedia data services a potentially attractive early option for support by the target network architecture.

  Several different capabilities and services fall under the category of multimedia services. A previous section discussed the recommendation for integrated transmission media. This section discusses some of the alternatives under consideration at the application and service layers.

  Computer Telephony Integration (CTI) is one of the fastest growing technology and product areas. With today's technology, it is no longer necessary to always build a local telephone infrastructure and a network infrastructure. Telephones can plug into network outlets or directly into the computer. Alternatively, telephones can be replaced by multimedia-equipped computers. Calls initiated from the data network can be routed over the data network or over the telephone network, depending on the performance, cost, or policies of the agency.

  Video conferencing and desktop collaboration tools and servers need to be provided by the network. While freeware products such as Microsoft NetMeeting work well, the network needs to provide servers and gateways for the best performance. Each capability also needs to be evaluated in terms of network resources required and QoS.

- **Integrated Network and Configuration Management** - As previously described, numerous systems and tools are currently required to manage and monitor FEMA networks. While tools need to be independently evaluated, the target architecture needs to have an integrated network and configuration management capability. Additional network management features that are being considered include:

  - Web-based network management status information
  - Automated IP address management
  - Large screen display facility
  - Automated discovery of network configuration changes
  - Correlation of multiple alarms
  - Automated configuration management.

- **Internet Call Center** - An Internet call center can potentially expand the reach and service of higher-level FEMA functions. Standard services and services tailored to specific scenarios or disasters can be designed. Initially, links can be provided between the current and Internet call centers. Eventually, the call centers should be completely integrated to provide the full range of functions from internal support to disaster services.

- **Alternate Access Methods** - Alternative access technologies such as Frame Relay, ATM, xDSL, and dial-up will continue to be investigated to determine if more cost-effective alternatives could be employed without impact to the mission or flexibility. The standard T1 access strategy works well but may be less cost effective than other alternatives, particularly if the connections need to remain in place for undefined timeframes after the initial installation.

3.5 Recommended Implementation Strategy

The FEMA network architecture implementation strategy includes a phased evolutionary approach, prototyping, legacy support, and an event-driven milestone schedule.

3.5.1 Phased Evolutionary Approach

The implementation of the target architecture is being carefully designed to meet FEMA requirements and objectives. A low risk, no downtime approach can be achieved with the use of a limited introduction and overlapping (hybrid) strategy.

As shown in Figure 3-10, certain technologies are being considered for introduction in the core, evaluated, and then transitioned to the Regions and field locations. The decision to transition from the core outward will be evaluated on a case-by-case basis. Subject to further engineering analysis, FEMA is planning that the integrated backbone technology be introduced initially in the core of the network. This approach will include selected locations at the top of the network hierarchy including Mt. Weather, Denton, Headquarters, and Denver.

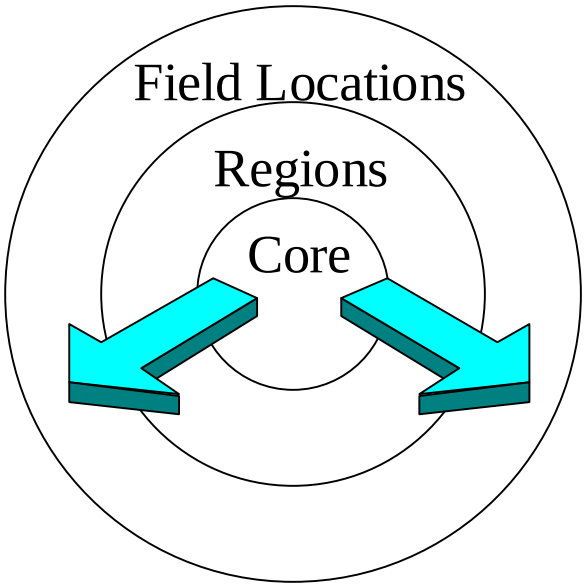

Figure 3-10. Phased Approach Alternative

The primary rationale for introducing integrated backbone technology in the core is the potential for higher bandwidth, more aggregated multimedia traffic, and centralized QoS management. In addition, integrated backbone technology may not be necessary or desired at all locations. Finally, the cost/benefit performance can be determined in a limited implementation before spreading the technology further.

Due to the nature and history of the voice network, careful planning and engineering must be conducted to ensure voice traffic is given appropriate priority and QoS. Similarly, the data bandwidth allocations must be engineered to adequately handle average and peak traffic patterns, as well as mission-critical applications such as NEMIS.

While the integrated backbone technologies are being evaluated for introduction in the core first, other technologies such as multimedia servers or Virtual Private Networks (VPNs) may well be easier to evaluate or provide better performance with a Regional or field implementation. In consultation with the Regions, the ITS Directorate may propose to begin the implementation outside the core due to availability of services, resources, or regional requirements. The results of regional and field implementations can then be evaluated for implementation in the core.

In addition to the phased approach, an overlapping or hybrid strategy is also possible for technologies in the backbone and other critical areas. The hybrid strategy would allow the technology to be introduced with minimal impact to the existing mission and architecture. The hybrid approach would allow operations, management, and support to be thoroughly evaluated prior to full cutover. Cutover to the new technology would then occur after FEMA has accepted the cost/benefit and risk assessment. As an alternative, the hybrid strategy could be maintained indefinitely to provide alternate routing or a cost-effective bandwidth overflow. Figure 3-11 illustrates a candidate phased, hybrid implementation strategy using ATM as the integrated backbone technology.

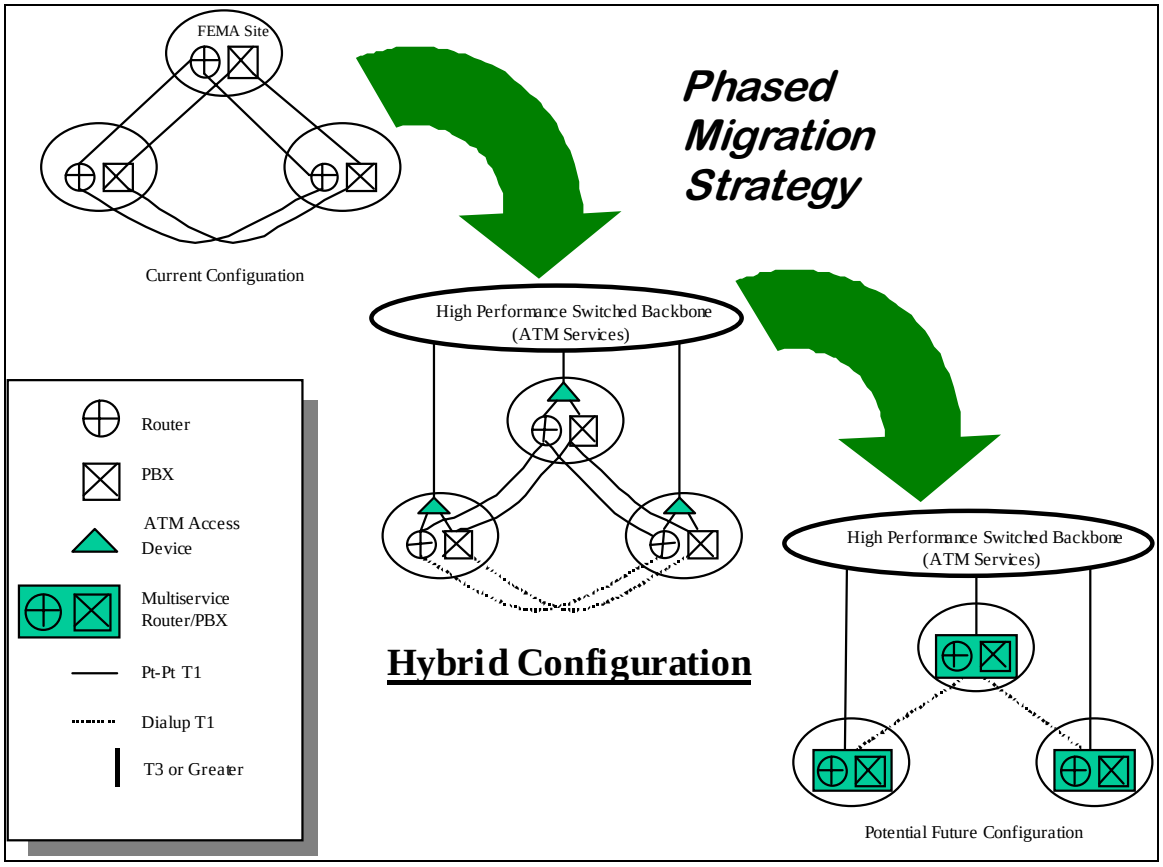

Figure 3-11. Hybrid Implementation

3.5.2 Prototyping

As an important architectural consideration, FEMA appreciates that vendor specifications and equipment interoperability are difficult to appraise on paper and in limited demonstrations. Consequently, FEMA plans to conduct extended evaluations of new technologies in prototype implementations.

Prototypes will be setup and evaluated in production environments so that cost, performance, and support issues can be realistically evaluated. The prototypes will also be structured to be easily disabled, without impact to the network, during the evaluation period. When the evaluation is complete, the intent is that a prototype can be expanded, removed, left in place or replaced with upgraded equipment. Figure 3-11, illustrates a hybrid implementation concept that can simplify removal or replacement of prototype equipment. For simplicity, only three sites are shown.

In migration to the target network architecture, evaluation plans and procedures will be developed to guide the prototype evaluation process. New technologies, such as ATM, will be evaluated for the full range of expected employment. Features such as Switched Virtual Circuits (SVC), Permanent Virtual Circuits (PVC), and QoS will be analyzed prior to prototyping to determine the preferred implementation and evaluation strategy.

Given the success or failure of the prototype evaluations, FEMA will be able to make informed cost/benefit decisions about full-scale implementations. Evaluation criteria and risk assessments developed in earlier phases will support the selection of technologies and vendors. Network architecture evaluations will help identify the appropriate locations, configuration, detailed systems engineering requirements, and schedule of network modifications.

3.5.3 Legacy Support

At each phase of the network architecture migration, it will be important to maintain legacy systems and networking support. The architecture must support legacy equipment until FEMA consciously and deliberately decides to phase out the legacy systems and equipment.

Prototype evaluations and vendor selection criteria will be developed with legacy support considerations of paramount importance. Because existing PBXs, routers, switches and associated software cannot be replaced immediately, test plans will be developed to address interoperability issues. Problem detection, troubleshooting and resolution procedures must be thoroughly tested. Test cases must be developed to stress the network, particularly the interfaces between new technology and legacy equipment.

3.5.4 Event-Driven Milestone Schedule

The FEMA ITS Directorate appreciates that a schedule-driven integration is difficult to achieve with low risk, particularly in an environment with fluctuating budgets. An important architectural consideration is that new technology should be evaluated, prototyped, and phased into the target architecture. As a result, an event-driven implementation strategy is under development and consideration. Section 3.4.2 summarized the most important objectives and criteria. Other significant factors that FEMA is considering in the development of the event-driven milestone schedule are outlined below:

- Independent technology evaluations
- Infrastructure preparations
- Vendor demonstrations
- Initial prototype
- Extended prototype in production environment
- Phased implementation plan (core, region, field)
- Legacy interoperability testing
- Potential for establishing partnerships with universities and other Federal agencies on the Next Generation Internet (NGI) and Internet2
- Potential for cooperative telecommunications buying services with other Federal agencies.

This page intentionally left blank

4 Maintaining and Implementing the *FEMA IT Architecture*

4.1 Introduction

This section provides a discussion of the activities that are required to maintain and implement the *FEMA IT Architecture*. This section also describes the maintenance process in terms of the organizational responsibilities and the change control process. The relationship of legacy systems and new systems to the maintenance and implementation of the *IT Architecture* is also identified. This section discusses two major requirements. These requirements are:

1) The need to maintain and update the IT and network architecture

2) The need to implement architectural components in new systems, in re-engineered legacy systems, and re-hosted systems.

In maintaining and implementing the *FEMA IT Architecture*, the principles provided in Appendix H shall apply.

4.2 Requirements and Plans for Maintaining and Implementing the IT Architecture

The following activities affect the maintenance and implementation of the *FEMA IT Architecture*. These activities are not only applicable to the architecture document itself, but also to the associated *IT Architecture* Data Base. A change in any one of the following activities may necessitate a change to the *IT Architecture* and the associated Data Base:

- A change in plans such as the *FEMA Strategic Plan*, the *Federal Response Plan*, the *National Mitigation Strategy*, or the *Annual Performance Plan*
- Introduction of new IT or network technologies
- Identification of new standards or standard tools
- A change to any FEMA organizational unit mission or business functions
- Identification of new opportunities for systems or applications
- A change in the informational flows of any FEMA organizational unit
- A change in the informational flows and IT infrastructure of a FEMA enterprise business partner to the extent that it has not been standardized and impacts FEMA IT systems
- The addition or deletion of documents or data stores to a FEMA organization unit
- Changes in plans, policies, and procedures resulting from activities for information assurance as part of Critical Infrastructure Protection (CIP)
- Issuance of new laws, directives, and court proceedings that affect the maintenance and implementation of the enterprise *IT Architecture*.

4.2.1 FEMA IT Architecture Change Management

The *FEMA IT Architecture* is intended to be relatively stable and evolve slowly over time. The architecture is intended to provide a stable and disciplined baseline for the development and implementation of conforming IT systems. Accordingly, major changes to the architecture can expect to be made relatively infrequently.

The ITS Directorate is designated as the primary development and management authority for the *FEMA IT Architecture*. Lead development responsibility is assigned to the ITS Management Division with the close cooperation and assistance of the Program Management Group, the Operations Division, and the Engineering Division. The Configuration Management (CM) Branch within the Management Division is responsible for the *mechanics* of maintaining configuration management controls over the *IT Architecture*, including document integrity, data base integrity, and digital signature controls. The CM Branch has distributed draft detailed procedures for configuration management to IRB and ISPAG members, which will also be used for maintenance of the *IT Architecture* baseline. This draft includes the establishment of a Technical Review Committee, chaired by the Director of the Engineering Division, ITS, and a Configuration Control Board (CCB), chaired by the CIO.

4.2.2 Plans for Implementation of the *FEMA IT Architecture*

To implement the target *IT Architecture* vision, the CIO and the ITS Directorate have determined that two ancillary, enterprise-wide guidance documents are necessary. These documents are:

1) ***FEMA Information Resources Management Policy and Procedural Directive (FIRMPD).*** This document already exists but will be rewritten to provide detailed policy and procedural guidance to be compatible with this *IT Architecture*.

2) ***IT Capital Planning and Investment Guide.*** A draft of this document also exists and will be rewritten to conform to the requirements of the *IT Architecture*.

4.2.3 Legacy Systems Integration

This *FEMA IT Architecture* recognizes that FEMA has a significant investment in legacy systems. It also recognizes that the current IT architecture is substantially meeting current operational requirements. This *FEMA IT Architecture* document sets forth the firm directive that the operation of legacy systems shall not be compromised or jeopardized merely to bring legacy systems into compliance with the Architecture. Rather, legacy systems shall be migrated to the target architecture in due consideration of the following major factors:

- What are the necessary resources needed to accomplish the migration and how do they compare against competing requirements?
- What is the lifetime remaining for the legacy system?
- Are underlying business functions and functional requirements stable?
- What is the operational demand for migration?
- What are the projected cost-benefit savings for migration?
- Is the return on investment for migration justifiable?
- What is the impact on other IT systems?
- What is the projected impact on FEMA networks and communications?
- What is the projected impact on enterprise resources such as personnel, training, hardware, software, data bases, etc.?
- Do FEMA's enterprise partners support the migration?
- Does the proposed migration support evolving mission needs?
- Is the proposed migration in conformance with FEMA IT architectural principles in Appendix H ?

4.2.4 CIO and IRB Guidelines for Re-Engineering of Legacy Systems

The CIO and IRB strongly encourage initiatives to re-engineer legacy systems to bring them into compliance with the *IT Architecture*. An organizational element may propose a re-engineering or re-hosting effort for a legacy system. The proposal should be forwarded to the CIO for consideration through normal business channels. The following guidelines apply:

- The proposal should indicate compliance with the *FEMA IT Architecture* and the architectural principles in Section 1.8. All deviations and exceptions should be noted.

- The proposal should address the questions in Section 4.2.3 to the satisfaction of the CIO and the IRB. The CIO may request that the proponent make a presentation to the IRB describing the initiative and addressing mechanisms for funding it.

- The proposal should indicate compatibility and compliance of the proposed effort with the National Emergency Management Information System (NEMIS) as an architectural cornerstone. Any proposed deviations and exceptions from the NEMIS approach shall be justified.

- The proposal should clearly address requirements and plans for cutover and transition to ensure continuity of operations.

4.2.5 NEMIS as a FEMA Architectural *Cornerstone*

FEMA has made a significant investment in the development and implementation of NEMIS. FEMA senior management clearly seeks to leverage this investment across the enterprise. In the development of NEMIS, emphasis has been placed on implementation and integration of advanced information technology components. NEMIS has provided a vehicle for FEMA to develop enterprise-wide capabilities with the potential for significant re-use.

The NEMIS project is dedicated to evolve as business functions, information flow requirements, enterprise-wide documents/data, and technology evolve. This *FEMA IT Architecture* clearly defines NEMIS as an architectural cornerstone within FEMA. All future IT developments, networking, re-engineering, and re-hosting shall be compatible with the *FEMA IT Architecture*. This means that consideration must be given to maintaining architectural compatibility with NEMIS or to working closely with the CIO to effect any substantive architectural changes in a mutually agreeable manner. The *FEMA IT Architecture* is open to good ideas and innovation produced by other enterprise systems.

4.2.6 Personnel Requirements for Development, Maintenance, and Implementation of the *FEMA IT Architecture*

Trained and knowledgeable personnel are considered vital for developing, maintaining, and implementing this *FEMA IT Architecture*. Within the ITS Directorate, persons assigned the task of developing, maintaining, and implementing the *IT Architecture* need the following major skills:

- Understanding of legal requirements contained in public law, directives, and court decisions and their potential impact on IT and NT systems
- Understanding of open systems standards and their implementation
- Clear insight into the FEMA organizational structure and its dynamics
- Established working relationships and partnerships with other Federal agencies, industry, and academia
- In-depth understanding of IT and NT architectural components including business functions, information flows, systems and applications, data and documents, security requirements and services, and advanced technologies
- Understanding of legacy systems at FEMA
- Strong communications skills and ability to bridge FEMA organizational elements in a congenial and cooperative manner to effect beneficial change.

4.2.7 IT Industry Coordination and Liaison

Maintenance and implementation of the *FEMA IT Architecture* demand close IT industry coordination and liaison: 1) to identify emerging opportunities, 2) to assess the state-of-the-art, 3) to maintain awareness of industry directions, and 4) to make FEMA's IT requirements clearly known to industry. Consistent with procurement regulations, security, privacy, and confidentiality agreements, this *IT Architecture* clearly sanctions external industry consultation and outreach activity toward the goals of adopting the best technology for FEMA enterprise-wide architectural components and protecting the critical information technology infrastructure.

4.2.8 Partnership with Other Federal Agencies, State, and Local Governments, and Voluntary Organizations

FEMA has a large number of partnerships with other Federal agencies, State, and local government; as well as with voluntary organizations. The *IT Architecture* supports these partnerships and encourages an expansion of the dialog. In particular, the *IT Architecture* encourages additional discussion in the following major areas:

- Potential for increased connectivity via Virtual Private Networks (VPNs) and Extranets
- Agreement on document and data formats (particularly for open systems formats)
- Consensus on standards and standard tools
- Streamlining of information flows to automate wherever possible
- Agreement on electronic information interchange requirements supported by digital certificate services
- Cost-sharing of IT systems, networking, and communications
- Improved methods for maintaining security and document/data integrity
- Improved methods for exploiting the Global and National Information Infrastructure
- Improved approaches and concepts for protecting critical cyber systems and networks
- Increased use of common COTS tools and products
- Shared understanding of the long-term legal and regulatory implications of advanced IT technology
- Sharing of IT lessons learned.

4.2.9 Understanding of Standards

In general, development and maintenance of the FEMA Technical Reference Model and Standards Profiles requires an in-depth and comprehensive understanding of a significant number of information and network standards. It is important to understand the capabilities and limitations of the standards as well as their future direction. An in-depth understanding of the standards is needed to assess Commercial Off-The-Shelf (COTS) implementations as well as to provide a basis for evaluating vendor and contractor proposals. In the system engineering process, an in-depth understanding of standards is also needed to properly specify requirements and not misuse the standard.

This *FEMA IT Architecture* supports collaboration of FEMA's IT professional staff with various standards development committees and authorities to gain increased awareness of standards activities, their direction, and key integration issues. This reflects FEMA's role across the emergency management community as a consumer of standards vice a developer. Participation and collaboration must be approved on a case-by-case basis by the CIO and shall be commensurate with the individual's workload and assigned job responsibilities.

4.2.10 Strategy and Plans for Hiring, Training, and Professional Development

The *IT Architecture* requires trained and knowledgeable IT professionals capable of working within the lifelines of the enterprise. The high-level strategy and plans for hiring, training, and professional development are briefly summarized as follows:

- To the maximum extent practicable, *IT Architecture* maintenance and implementation responsibilities will be assigned to current staff members in the ITS Directorate.

- Individuals who are assigned *IT Architecture* maintenance and implementation responsibilities are encouraged to request additional training as needed.

- All FEMA organizational elements that have significant IT and network development, operations, and/or maintenance responsibilities will ensure that any future hiring or staffing will incorporate personnel requirements and evaluation factors commensurate with this *IT Architecture*.

4.2.11 Seat Management

One ancillary goal of the *FEMA IT Architecture* is the anticipation that the architecture will establish the primary vehicle for the FEMA ITS Directorate to explore seat management.

Seat Management provides a unified service in the way FEMA currently buys desktop computers and support services. Services are paid for on a per seat basis. The seat management concept can allow FEMA to keep pace with technology, eliminate different sources of hardware and software, integration, help desk and other services, and improve security and reliability. This *FEMA IT Architecture* document supports seat management as an accepted and standardized approach to acquisition of IT resources and architectural components.

4.2.12 Employment of Agency Resources vs. Outsourcing

It is a goal of this *IT Architecture* that maintenance and implementation activities shall be performed by Agency personnel wherever practicable. Contractor support may be required and will be approved or concurred with on a case-by-case basis by the CIO.

4.2.13 CIO Policies for the *IT Architecture*

4.2.13.1 CIO Policy on Compliance, Waivers, and Certification

The CIO has determined that compliance with this *IT Architecture* is mandatory for the development of new IT systems and any proposed re-engineering, re-hosting, or additional development of legacy systems. The CIO has also determined that the architectural principles as stated in Section 1.8 must be followed for FEMA's IT systems. Compliance with the architectural principles shall be verified in all IT systems reviews and audits.

4.2.13.2 CIO Policy on Configuration Management, Configuration Audits, and Configuration Control

The CIO has determined that FEMA shall implement standardized CM services that shall be mandatory for all IT systems to which this architecture applies. The FEMA ITS Directorate has developed a draft set of policies and procedures for configuration management entitled *Draft Technical Review Committee (TRC) and Configuration Control Board (CCB) Guidelines*, dated May 4, 1998. This document is expected to become the basis for disciplined enterprise-wide configuration management. Major CM activities shall include: configuration identification, configuration assessment and establishment of baselines, configuration controls, configuration status accounting, and configuration audits. Automated CM tools will be used as appropriate.

As a matter of policy, CM shall be applied in a disciplined and standardized manner across the lifetime of IT systems, networks, data stores, enterprise documents, metadata, business functions, and selected architectural components (such as digital certificates for digital signature).

4.2.13.3 CIO Policy on Allowable Systems Engineering Approaches

As a matter of policy, the CIO has determined that new systems development and any re-engineering or re-hosting shall be performed in accordance with an established and recognized FEMA life-cycle model. All new proposed projects must identify the planned life-cycle model and any planned tailoring. The CIO, in consultation with the IRB, shall verify the assignment of the life-cycle model. On a case-by-case basis, and particularly for mission-critical systems, the CIO may mandate that the proposed project office use formal Software Engineering Institute (SEI) criteria for development.

4.2.13.4 CIO Policy on Information Protection and Security

As a matter of policy, the CIO has determined that information protection and security are a vital component of FEMA IT systems or network development, integration, maintenance, and operations. As a matter of high priority, FEMA is currently addressing the requirements for Critical Infrastructure Protection as mandated by EO 13010 and PDD-63. All IT systems and networking development, integration, maintenance, and operations shall be compliant with the approved FEMA Security Architecture that results from that effort.

Go to Appendices